BCH符号（その２）

情報数理学特別講義I 第8回

2025-11-06

復習：生成多項式の根による巡回符号のパリティ検査行列

次数 r の生成多項式 $g(x)$ で定義される巡回符号 $\mathcal{C}$ のパリティ検査行列 H は，$g(x)$の根を用いて定義できる．巡回符号の性質より，符号多項式 $c(x)$ は $g(x)$ を因数に持つので，$g(x)$ の r 個の根 $x_1, x_2, \ldots, x_r$ について $c(x_i) = 0$ が成り立つ．
これを行列で表すと，

$$H\underline{c}^T = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_r & x_r^2 & \cdots & x_r^{n-1} \end{pmatrix} \underline{c}^T = \underline{0}.$$

ただし $\underline{c} = (c_0, c_1, \ldots, c_{n-1})$ で符号多項式 $c(x)$ の係数を要素にもつベクトルである．

生成多項式 $g(x) = 1 + x + x^3$ で定義される巡回符号の符号語 $\underline{c} = (1, 0, 1, 1, 1, 0, 0)$ について，多項式による根の評価とパリティ検査行列の等価性を確かめよう.
いま，$g(x)$ の根を α とすると，符号語 $\underline{c}$ に対応する符号多項式 $c(x) = 1 + x^2 + x^3 + x^4$ も α を根にもつ．さらに，$GF(2^3)$ 上では α^2 も根となる.
ただし $GF(2^3)$ を構成する原始多項式は $p(x) = 1 + x + x^3$ である.

練習問題1(10分)

(1) $c(x)$に α と α^2 を代入して，$c(\alpha) = c(\alpha^2) = 0$ となることを確かめよ.
(2) 生成多項式の根である α と α^2 を用いたパリティ検査行列Hを構成せよ.
(3) さらにそのパリティ検査行列 H に符号語 $\underline{c}$ をかけて，$\underline{0}$ になることを確かめよ.

$$c(x) = 1 + x^2 + x^3 + x^4$$

$$\underline{c} = (1, 0, 1, 1, 1, 0, 0)$$

ヴァンデルモンド行列とその性質

ヴァンデルモンド行列の行列式について，次の定理が成り立つ.

定理 8.1

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le j < i \le n} (x_i - x_j).$$

この定理から導かれる重要な性質：

$x_1, x_2, \ldots, x_n$ が相異なる元であれば行列式が非ゼロになるため，
n 個の行（列）ベクトルは線形独立.

前回述べた巡回符号の最小距離に関する **定理 8.2** の言い換え
位数が n である任意の元 $\beta \in GF(2^q)$ に対して，指数部が d 個連続している $\beta, \beta^2, \ldots, \beta^d$ を全て根に持つ生成多項式 $g(x)$ で定義される巡回符号の最小距離は $d+1$ 以上となる.

カジュアルな証明
生成多項式 $g(x)$ が 指数部が d 個連続した元を根に持つ.
$\Rightarrow$ パリティ検査行列の任意の d 列からなる部分行列がヴァンデルモンド行列となるため，どの d 列も線形独立つまり，d 個の列ベクトルの和は必ず非ゼロになる（パリティ検査行列を満たさない）.
$\Rightarrow$ $g(x)$ で定義される巡回符号は重み d （d 個が 1 であるような）符号語を持たない.
$\Rightarrow$ この巡回符号の最小距離は $d+1$ 以上である.

BCH符号

$GF(p)$上の巡回符号の代表である符号 Bose-Chaudhuri-Hocquenghem (BCH) 符号
は次のように定義される.

定義：BCH符号
α を $GF(p^q)$ の原始元とする. このとき $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$ の全てを根とする $GF(p)$ 上の生成多項式 $g(x)$ により定義される $GF(p)$ 上の符号長 $n = p^q - 1$ の巡回符号を
BCH符号（t 誤り訂正BCH符号）という.

BCH符号の生成多項式 $g(x)$ とその次数

$\alpha^i \in GF(p^q)$ の $GF(p)$ 上の最小多項式を $\mu_{\alpha^i}(x)$とすれば，BCH符号の生成多項式は，

$$g(x) = \mathrm{LCM}\left(\mu_{\alpha^1}(x), \mu_{\alpha^2}(x), \ldots, \mu_{\alpha^{2t}}(x)\right)$$

となる．ただし LCM は最小公倍数を表す．

これと定理 8.2 から，BCH 符号の最小距離 d は $d \geq 2t+1$ を満足する．
このとき，$2t+1$ のことを「設計距離」という．また定理 8.4 から，α^i の最小多項式について $\deg \mu_{\alpha^i}(x) \leq q$ が成り立つので

$$\deg g(x) \leq 2qt$$

が成り立つ．

BCH符号の生成多項式 $g(x)$ とその次数（続き）

特に $p = 2$ のときは，定理 8.3 から α^i と α^{2i} の最小多項式は一致するので

$$g(x) = \mathrm{LCM}\{\mu_\alpha(x), \mu_{\alpha^3}(x), \ldots, \mu_{\alpha^{2t-1}}(x)\}$$

としても良い．この場合

$$\deg g(x) \leq qt$$

が成り立つ．
従って，2元 BCH 符号の次元 k は $n - qt$ 以上である．

BCH符号のパラメータまとめ

以上をまとめると，BCH符号のパラメータについて以下の表のようになる.

	$p=2$	$p\neq 2$
符号長 n	$n=2^q-1$	$n=p^q-1$
メッセージ長(次元) k	$k\geq n-qt$	$k\geq n-2qt$
パリティ長 $n-k$	$n-k\leq qt$	$n-k\leq 2qt$
最小距離 d	$d\geq 2t+1$	$d\geq 2t+1$

ただし q は原始元 α を定義する $GF(p^q)$ の指数である.

例題

訂正数 $t=2$ の時，2元BCH符号の生成多項式の次数は？

長さ 15 の2元BCH符号を作ってみよう.

α を $GF(2^4)$ の原始元とする. ただし $GF(2^4)$ を構成する原始多項式は $p(x) = 1 + x + x^4$ である.

BCH符号の生成行列の構成法 $g(x) = \mathrm{LCM}\{\mu_\alpha(x), \mu_{\alpha^3}(x), \ldots, \mu_{\alpha^{2t-1}}(x)\}$ より

$$
\begin{aligned}
t = 1 &: g(x) = \mu_\alpha(x) = 1 + x + x^4 \\
t = 2 &: g(x) = \mathrm{LCM}\{\mu_\alpha(x), \mu_{\alpha^3}(x)\} = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4) \\
&\quad = 1 + x^4 + x^6 + x^7 + x^8 \\
t = 3 &: g(x) = \mathrm{LCM}\{\mu_\alpha(x), \mu_{\alpha^3}(x), \mu_{\alpha^5}(x)\} \\
&\quad = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)(1 + x + x^2) \\
&\quad = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}
\end{aligned}
$$

長さ 15 の2元BCH符号のパリティ検査行列

$t = 1$ のとき

生成多項式が $\mu_\alpha(x)$ であることから，α を根に持つ．よってパリティ検査行列は

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

1行目は $GF(2^4)$ の元を行列の要素とした表記.

2行目は $GF(2)$ の元を行列の要素とした表記（２元行列）.

1行目でパリティ検査行列との積を計算する際には，$GF(2^4)$ 上の計算になり，2行目のパリティ検査行列を用いて積をとる際には $GF(2)$ 上の計算をすればよい（いずれも等価）

$t = 2$ のとき
生成多項式が $\mathrm{LCM}\{\mu_\alpha(x), \mu_{\alpha^3}(x)\}$ であることから，α と α^3 を根に持つ.
よってパリティ検査行列は

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

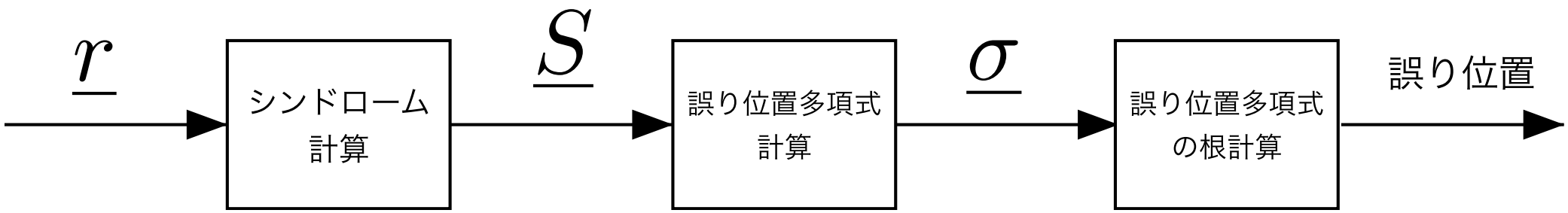
練習問題2(5分)

$t = 3$ のときのパリティ検査行列を求めよ.
ただし，要素は $GF(2^4)$ の元として表現すること．※2元行列じゃなくてよい.

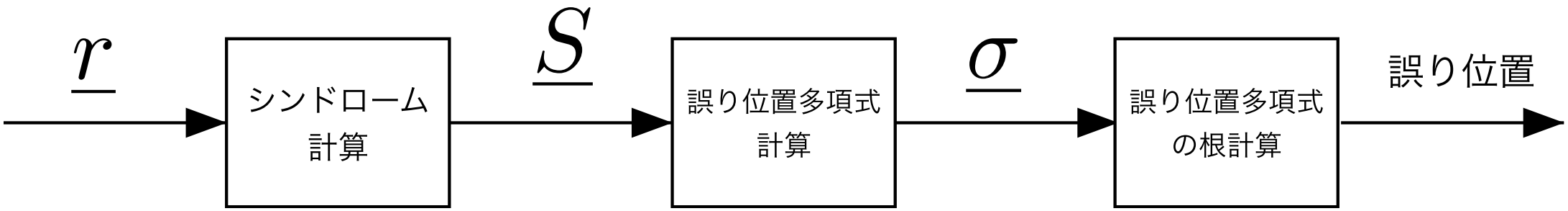
2元BCH符号の復号法（誤り訂正のしかた）

2元BCH符号の復号は以下の3ステップで行う.

1. 誤りを含む可能性のある受信語 $\underline{r}$ を入力し，シンドローム $\underline{S}$ を計算する.
2. シンドローム $\underline{S}$ から，誤り位置多項式 $\sigma(x)$ を求める.
3. 誤り位置多項式 $\sigma(x)$ の根を計算する.



2元BCH符号の復号法（誤り訂正のしかた）



シンドローム $\underline{S}$ とは，**生成多項式が持つ根を受信多項式に代入した際に得られる値**．つまり $\underline{S} = \left(r(\alpha), r(\alpha^3), \cdots, r(\alpha^{2t-1})\right)$．誤りがない場合，$\underline{S} = \underline{0}$ となる．

誤り位置多項式 $\sigma(x)$ は，誤**り位置に対応する元 α^i を根とする多項式**で，シンドローム $\underline{S}$ から求めることができる．誤り位置多項式の次数は誤りの数に等しい，t 誤り訂正BCH符号の場合，誤り位置多項式の次数は最大で t となる．

$t = 1$ の場合

いま，i ビット目に誤りが生じた受信多項式 $r(x)$ を考える．
生成多項式 $g(x) = 1 + x + x^4$ の根 α を受信多項式 $r(x)$ に代入し，シンドロームを評価すると．受信多項式 $r(x)$ は符号多項式 $c(x)$ と 誤り多項式 $e(x)$ の和であるから，

$$\begin{aligned} r(\alpha) &= c(\alpha) + e(\alpha) \\ &= g(\alpha) \cdot m(\alpha) + e(\alpha) \\ &= e(\alpha) \end{aligned}$$

となる．i ビット目に誤りが生じたエラー多項式は $e(x) = x^{i-1}$ であることから，シンドロームは $S_1 = r(\alpha) = \alpha^{i-1}$ となる．
よって得られたシンドローム S_1 の**指数部**を見ることで，誤り位置を特定することができる．
誤り位置が原始元 α のべきに対応している点がポイント！
※以降，α^j を受信多項式に代入して得られるシンドロームを S_j とする．

練習問題3(10分)

以下の受信多項式の誤り位置（何ビット目が誤りか）を求めよ.

(1) $r(x) = 1 + x + x^2 + x^4 + x^5$

(2) $r(x) = 1 + x^3 + x^4 + x^6$

$t = 1$ の2元BCH符号で2ビット誤りが発生すると？

$t = 1$ の2元BCH符号で2ビット誤りが発生すると？

誤り位置と異なるビットを反転してしまう．このことを**誤訂正**と呼ぶ．

i と j ビット目に誤りが発生すると，誤り位置多項式は

$$e(x) = x^{i-1} + x^{j-1}$$

となり，シンドローム S_1 は

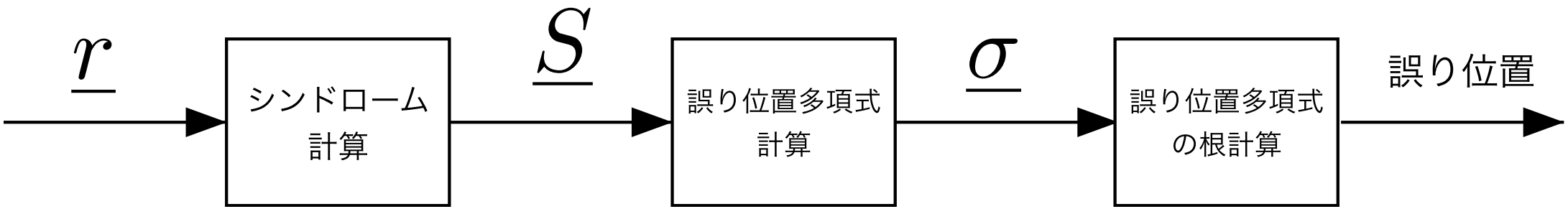
$$S_1 = e(\alpha) = \alpha^{i-1} + \alpha^{j-1} = \alpha^{k-1}$$

となるため，異なるビット位置 k を反転してしまう．
2元BCH符号は，基本的には設計距離 t を超える誤りを訂正することはできない．
t を超える誤りが生じた際には，誤訂正が生じ，誤りを増やしてしまう．

$t = 2$ の場合

$t = 2$の訂正方法を，先に述べた2元BCH符号手順に従い説明する.

1. 誤りを含む可能性のある受信語 $\underline{r}$ を入力し，シンドローム $\underline{S}$ を計算する.
2. シンドローム $\underline{S}$ から，誤り位置多項式 $\sigma(x)$ を求める.
3. 誤り位置多項式 $\sigma(x)$ の根を計算する.



シンドロームの計算 $(t = 2)$

$t = 2$ の2元BCH符号の生成多項式は α と α^3 を根に持つため，2つのシンドローム S_1, S_3 を計算することができる.
いま，$i + 1$ と $j + 1$ ビット目に誤りが発生したとする．このときのエラー多項式は $e(x) = x^i + x^j$ となる．よって得られるシンドロームは

$$S_1 = \alpha^i + \alpha^j,$$
$$S_3 = \alpha^{3i} + \alpha^{3j}$$

となる.
2つの未知変数 i, j に対して，2つの式を得ることができるため，解くことができそうだが，i, j が指数部であるため，単純な2次方程式では解くことができない.
どうするか？

誤り位置多項式(Error Locator Polynomial: ELP)

ここで，誤り位置に対応する元(Error Locator) を根にもつ誤り位置多項式 $\sigma(x)$ を考える.
誤り位置多項式 $\sigma(x)$ は α^i と α^j を根に持つので

$$\sigma(x) = (x - \alpha^i)(x - \alpha^j)$$

と表せる.

復号器の入力である受信多項式から得られる**シンドローム** S_1, S_3 でこの誤り位置多項式 $\sigma(x)$ を表すことを考えよう.
α^i, α^j で直接立式すればいいじゃんと思うかもしれないが，誤り訂正する際に誤り位置に対応する i, j は未知変数のため，α^i, α^jは直接使用できない点に注意しておいてほしい.
平たく言うと，誤り訂正とは，シンドローム与えられるが，α^i, α^j は与えられない.

$S_1 = \alpha^i + \alpha^j$ より

$$\begin{aligned}\sigma(x) &= \alpha^i\alpha^j - (\alpha^i + \alpha^j)x + x^2 \\ &= \alpha^i\alpha^j - S_1 x + x^2\end{aligned} \tag{9-1}$$

$\alpha^i\alpha^j$ は計算できるか？

$$\begin{aligned}S_1^3 &= (\alpha^i + \alpha^j)^3 \\ &= \alpha^{3i} + \alpha^{2i}\alpha^j + \alpha^i\alpha^{2j} + \alpha^{3j} \\ &= \alpha^{3(i)} + \alpha^{3j} + \alpha^i\alpha^j\left(\alpha^i + \alpha^j\right) \\ &= S_3 + \alpha^i\alpha^j S_1\end{aligned}$$

よって

$$\alpha^i\alpha^j = \left(S_1^3 - S_3\right)S_1^{-1}.$$

これを式 (9-1) へ代入すると

誤り位置多項式の根を求める.

$$\sigma(x) = \left(S_1^3 - S_3\right) S_1^{-1} - S_1 x + x^2$$

となり，シンドロームからなる誤り位置多項式 $\sigma(x)$ が得られた.

$GF(2^4)$ の非零の元は高々15個なので，これらを全て $\sigma(x)$ に代入して，$\sigma(x)$ の根を求めることで，誤り位置を求めることができる.

練習問題4(15分)

$GF(2^4)$ の原始元 α の最小多項式 を $\mu_\alpha(x) = 1 + x + x^4$ とする．生成多項式 $g(x) = \mu_\alpha \mu_{\alpha^3}$ で定義された長さ 15 の2誤り訂正2元BCH符号によって符号化された
符号多項式が，通信路を通って受信多項式 $r(x) = 1 + x^2 + x^4 + x^9$ となったとき，
誤り位置に対応する$GF(2^4)$ 上の元を求めよ．

解法手順
(1) シンドローム S_1, S_3 を計算する．
(2) 誤り位置多項式 $\sigma(x) = \left(S_1^3 - S_3\right) S_1^{-1} - S_1 x + x^2$ を計算する．
(3) $GF(2^4)$ の非零の元を順に $\sigma(x)$ へ代入し，誤り位置多項式の根を求める．

演習

(1) $p(x) = 1 + x + x^4$ により構成された $GF(2^4)$ 上の原始元 α, ただし $p(\alpha) = 0$, を根に持つ生成多項式 $g(x)$ で定義された1誤り訂正2元BCH符号によって符号化された符号多項式が，通信路を通って受信多項式 $r(x) = 1 + x + x^2 + x^3 + x^5 + x^6 + x^8 + x^{10}$ となったとき，誤り位置に対応する$GF(2^4)$ 上の元を求めよ．ただし解答（誤り位置に対応する非零の元）だけでなく，解法手順と途中計算も書くこと.

メッセージ多項式は $m(x) = x^3 + x^5$ に対し，$p(x) = 1 + x + x^4$ により構成された $GF(2^4)$ 上の原始元 α, ただし $p(\alpha) = 0$, と α^3 を根に持つ生成多項式 $g(x)$ で定義される
2誤り訂正2元BCH符号の符号化を以下の２通りで行え.
(2) 非組織符号化により符号化する（ヒント：生成多項式を掛ける）
(3) 組織符号化により符号化する（ヒント：CRCの符号化）